Comment on "Quantum Key Distribution in the Holevo Limit"

In a Letter, Cabello [1] proposed a quantum key distribution (QKD) Protocol which attended to Holevo limit. He assumed that the quantum channel is composed of two qubits (1 and 2), and is prepared with equal probabilities in one of four orthogonal pure states $|\psi_i\rangle$ ($i = 0, 1, 2, 3$), and that Eve cannot have access to qubit 2 while she still holds the qubit 1. He considers the following states (for simplicity, we have replaced polarization states with spin states)

$$|\psi_0\rangle = |00\rangle_{12} \qquad |\psi_1\rangle = \frac{1}{\sqrt{2}}[|10\rangle_{12} + |01\rangle_{12}]$$
$$|\psi_2\rangle = \frac{1}{\sqrt{2}}[|10\rangle_{12} - |01\rangle_{12}] \qquad |\psi_3\rangle = |11\rangle_{12} \tag{1}$$

We use the states $|0\rangle$ and $|1\rangle$ to represent spin up and spin down respectively. The efficiency of a QKD protocol, E, is defined as [1]:

$$E = \frac{b_s}{q_t + b_t}, \tag{2}$$

where b_s is the expected number of secret bits received by Bob, q_t is the number of qubits used in the quantum channel, and b_t is the number of bits used in the classical channel between Alice and Bob. In Cabllo's scheme $b_t = 0$ and $q_s = q_t$, which leads to $E = 1$ (the Holevo limit). Cabello's protocol (CP) has some basic properties: (a) CP uses all of Hilbert space dimensions, (b) He has defined an interesting criterion for the efficiency of QKD protocols, (c) He avoids using classical channel.

Eve could use a simple plan to distinguish between (ψ_0, ψ_3) and (ψ_1, ψ_2), without being detected by Alice and Bob. In other words, the set of four states are now partitioned into two sets. To show this, we assume Eve's particle to be in the state $|0\rangle_e$. When the qubit 1 passes through the first channel, she applies a CNOT operation on the qubit 1, as the control qubit, and her own particle, as the target. Then, she lets the qubit 1 goes to Bob's system. When she receives the qubit 2, she does the same operation on it and on her own qubit. After this operations, we have:

$$|\psi_i\rangle|0\rangle_e \longrightarrow |\psi_i\rangle|0\rangle_e \qquad i = 0, 3$$
$$|\psi_i\rangle|0\rangle_e \longrightarrow |\psi_i\rangle|1\rangle_e \qquad i = 1, 2 \tag{3}$$

At this stage, there is a trick by which Eve can distinguish exactly between two of the four states [2]. After the application of the second CNOT, she makes a measurement on her own particle in the $\{|0\rangle, |1\rangle\}$ basis. If she gets $|1\rangle$, she would let the qubit 2 go to Bob's system. Otherwise, by a measurement on the qubit 2 in the $\{|0\rangle, |1\rangle\}$ basis, she could understand whether the state of Alice and Bob is $|00\rangle$ or $|11\rangle$. This means that an undetectable Eve can know Alice's encoding whenever Alice uses the basis (ψ_0, ψ_3), making the CP insecure.

In the BB84 [3] protocol, security is guaranteed by the no-cloning theorem in the non-orthogonal states. CP was founded on the no-cloning principle for orthogonal states, which was suggested by T. Mor [4]. He proposed that the two (or more) orthogonal states cannot be cloned, if the reduced density matrices of the first subsystem are non-orthogonal and non-identical and the reduced density matrices of the second subsystem are non-orthogonal. Here a basic question is whether no-cloning condition for non-orthogonal and orthogonal states is sufficient to have the security of QKD protocol? With attention to our Eavesdropping approach, it seems that Mor's arguments for no-cloning principal for orthogonal states [4] is not general enough to avoid eavesdropping. In what follows, we would like to show that our approach is not restricted to CP. For example, we consider two non-maximally entangled states as follows:

$$|\psi\rangle = \cos\alpha|0\rangle_1|1\rangle_2 + \sin\alpha|1\rangle_1|0\rangle_2$$
$$|\phi\rangle = \cos\beta|0\rangle_1|0\rangle_2 + \sin\beta|1\rangle_1|1\rangle_2$$

with $0 < \alpha, \beta < \pi/2$ and $\alpha \neq \beta \neq \pi/4$. The reduce density matrices for the first subsystems are: $\rho^1_\psi = \cos^2\alpha|0\rangle\langle 0| + \sin^2\alpha|1\rangle\langle 1|, \varrho^1_\phi = \cos^2\beta|0\rangle\langle 0| + \sin^2\beta|1\rangle\langle 1|$. These reduced density matrices are neither orthogonal nor identical, and so they could't be cloned, and the reduced density matrices for second subsystems are: $\rho^2_\psi = \cos^2\alpha|1\rangle\langle 1| + \sin^2\alpha|0\rangle\langle 0|, \varrho^2_\phi = \cos^2\beta|0\rangle\langle 0| + \sin^2\beta|1\rangle\langle 1|$. These reduced density matrices are not orthogonal to each other, but this protocol is not secured completely against a double CNOT operations.

Here are some questions: What are the defects in the Mor proposal? How Mor proposal can be repaired? In another paper in progress, we respond to these questions.

The authors are grateful to referee for useful comments and A. T. Rezakhani for critical reading.(this work is supported under project name: *Aseman*).

A. Fahmi[1] and M. Golshani[1,2]
fahmi@theory.ipm.ac.ir
[1]School of Physics, Institute for Studies in Theoretical Physics and Mathematics (IPM) P. O. Box 19395-5531, Tehran, Iran
[2]Department of Physics, Sharif University of Technology, P. O. Box 11365-9161, Tehran, Iran.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.65.Bz,89.70.+c

[1] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[2] The same defect exist at the G. L. Long and X. S. Liu, (Phys. Rev. A **65**, 32302 (2002)) paper.
[3] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175-179.
[4] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).